IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

No. 3:23-cv-176-PDW-ARS

In re Brady Martz Data Security Litigation

ORDER ADOPTING STIPULATION FOR ELECTRONICALLY STORED INFORMATION (ESI) PROTOCOL

Per the Stipulation of the Parties, the Court hereby enters the following Electronically Stored Information (ESI) Protocol order:

A. General Principles

1. The Parties will conduct discovery in a cooperative, collaborative, and transparent manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions. The Parties will meet and confer about discovery issues in an effort to avoid or resolve disputes without court intervention.

2. Parties may obtain all discovery regarding any nonprivileged matter that is relevant to any party's claim or defense. The Parties will also consider the proportionality standard embodied in Fed. R. Civ. P. 26(b)(1), which requires consideration of the importance of the issues at stake, the amount in controversy, parties' relative access to relevant information, parties' resources, and whether the burden or expense of the proposed discovery outweighs its likely benefit. To further the application of the proportionality

standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as practicable.

3. The Partes will consider and abide by the specific limitations on electronically stored information as set out in Fed. R. Civ. P. 26(b)(2)(C), including that a party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.

B. Definitions

a. "Document" is defined to be synonymous in meaning and equal in scope to the usage of this term in Rules 26 and 34 of the Federal Rules of Civil Procedure. The term "Document" shall include Hard-Copy Documents, Electronic Documents, and ESI, as defined herein.

b. "Hard-Copy Document" means Documents existing in paper form at the time of collection.

c. "Native Format" means and refers to the format of ESI in which it was generated and/or as used by the producing party in the usual course of its business and in its regularly conducted activities. For example, the native format of an Excel workbook is .xls or .xlsx.

e. "Metadata" means (i) information embedded in or associated with a native file that is not ordinarily viewable or printable from the application that generated, edited, or modified such native file which describes the characteristics, origins, usage, and/or validity of the electronic file; (ii) information generated automatically by the operation of

a computer or other information technology system when a native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system, (iii) information, such as Bates numbers, created during the course of processing documents or ESI for production, and (iv) information collected during the course of collecting documents or ESI, such as file names, file paths, system dates, name of the media device on which it was stored, or the custodian or noncustodial data source from which it was collected.

f. "Optical Character Recognition" or "OCR" means the process of recognizing and creating a file containing visible text within an image.

C. ESI Disclosures

Prior to conducting searches for ESI in response to discovery requests, and in conjunction with negotiations on discovery requests, each party shall disclose within a reasonable amount of time:

1. Custodians. A list of custodians most likely to have ESI relevant to this litigation in their possession, custody, or control. The custodians shall be identified by name and title,. and the parties may meet and confer to prioritize any such custodial production.

2. Non-Custodial Data Sources. A list of non-custodial data sources/databases (e.g., share drives, servers), if any, which likely contain ESI relevant to this litigation. Discovery related to non-custodial data sources may be phased and the parties may meet and confer to prioritize any such production.

3. Third-Party Data Sources. A list of third-party data sources, if any, likely to contain ESI relevant to this litigation (e.g., third-party email providers, mobile device providers, cloud storage) and, for each such source, the extent a party controls preservation of such information.

4. Inaccessible Data. A list of data sources, if any, which is likely to contain ESI relevant to this litigation (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

5. Foreign data privacy laws. Nothing in this Stipulation/Order is intended to prevent either party from complying with the requirements of a foreign country's data privacy laws, e.g., the European Union's General Data Protection Regulation (GDPR) (EU) 2016/679. The parties agree to meet and confer before including custodians or data sources subject to such laws in any ESI or other discovery request.

D. ESI Discovery Procedures

1. On-site inspection of electronic media. Such an inspection shall not be required absent a demonstration by the requesting party of specific need and good cause or by agreement of the parties.

2. Search methodology. The parties shall timely confer to attempt to reach agreement on appropriate search terms and queries, file type and date restrictions, data sources (including custodians), and other appropriate computer- or technology-aided methodologies, before any such effort is undertaken in order to identify ESI that is subject

to production in discovery and filter out ESI that is not subject to discovery. The parties shall continue to cooperate in an iterative process in negotiating and revising the appropriateness of the search terms and methodology.

3. This Stipulation does not preclude a Requesting Party from serving discovery seeking information about a Producing Party's network design, types of databases, database dictionaries, access control lists and security access logs and rights of individuals to access systems and specific files and applications, the ESI document retention policy, organizational chart for information systems personnel, or the backup and systems recovery routines, including, but not limited to, tape rotation and destruction/overwrite policy. This stipulation does not oblige a Responding Party to produce such information, unless otherwise requested in written discovery or deposition. Upon such request, the parties will meet and confer to determine the appropriate scope.

4. If after the parties have identified initial document custodians, and the requesting party believes that additional document custodians or sources should be added after reviewing the produced documents, then the requesting party shall advise the producing party in writing of the proposed additional document custodians or sources of data and the basis for such request. The Parties will meet and confer and if the parties are unable to agree to add the specified custodians or sources, the matter may be brought to the Court.

5. A producing party need not use a specific manner to collect and produce documents. A manual review for responsiveness and privilege may be utilized, whether or not search terms or technology-aided review is also utilized.

6. Format.

a. To the extent reasonably accessible and proportional to the needs of the case, ESI will be produced to the requesting party with searchable text and corresponding metadata when reasonably available, in an agreeable standard format to be decided between the parties. ESI shall be produced in PDF, native, or single-page TIFF files with extracted text, if available, and corresponding metadata in a load file in compliance with Section 9 below. Acceptable formats include, but are not limited to, native files, multi-page TIFFs (with a companion OCR or extracted text file), single-page TIFFs (only with load files for eDiscovery software that includes metadata fields identifying natural document breaks and also includes companion OCR and/or extracted text files), and searchable PDF.

b. Unless otherwise agreed to by the parties, files that are not easily converted to image format, such as spreadsheet (*e.g.*, XML), Power Point, database, and drawing files (*e.g.,* CAD), will be produced in native format.

c. Each document image file shall be named with a unique number (Bates Number). File names should not be more than twenty characters long or contain spaces. When a text-searchable image file is produced, the producing party must preserve

the integrity of the underlying ESI, i.e., the original formatting, the metadata (as noted below) and, where applicable, the revision history.

d. If a document is more than one page, the unitization of the document and any attachments and/or affixed notes (full families) shall be maintained as they existed in the original document.

e. The parties shall produce their information in the following format: single-page images and associated multi-page text files containing extracted text or with appropriate software load files containing all information required by the litigation support system used by the receiving party. If implementing a third-party ESI vendor, party's vendors are encouraged to communicate prior to production to ensure delivery specs are acceptable for the review software.

f. The full text of each electronic document shall be extracted ("Extracted Text") and produced in text file. The Extracted Text shall be provided in searchable ASCII text format (or Unicode text format if the text is in a foreign language) and shall be named with a unique Bates Number (e.g., the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

7. De-duplication. The parties may de-duplicate their ESI production across custodial and non-custodial data sources after disclosure to the requesting party, and the deduplicate custodian information removed during the de-duplication process shall be tracked in a duplicate/other custodian field in the database load file.

a. De-duplication shall be performed only at the parent document level so that the attachments are not de-duplicated against identical stand-alone versions of such documents and vice versa (*e.g.*, a standalone document that is also an attachment to an email should not be deduplicated);

b. Attachments to emails or other documents shall not be disassociated from the parent email or document, even if they are exact duplicates of another Document in the production; and

8. Email Threading. The parties may use analytics technology to identify email threads and need only produce the unique most inclusive copy and related family members and may exclude less inclusive email strings. Email thread suppression shall not eliminate the ability of the receiving party to identify every custodian who had a copy of the produced document or email, and the producing party will not remove from production any unique branches and/or attachments contained within an email thread.

9. Metadata fields. The parties agree that the following metadata fields should be produced, and only to the extent it is reasonably accessible and non-privileged: (i) document type; (ii) custodian and duplicate custodians (or storage location if no custodian); (iii) author/from; (iv) recipient/to, cc and bcc; (v) title/subject; (vi) email subject; (vii) file name; (viii) file size; (ix) file extension; (x) original file path; (xi) date and time created, (xii) sent, modified and/or received; (xiii) hash value; (xiv) document type; and (xv) email thread index. The list of metadata type is intended to be flexible and may be modified by further written agreement of the parties.

10. Hard-Copy Documents. If the parties elect to produce hard-copy documents in an electronic format, the production of hard-copy documents will include a cross-reference file that indicates document breaks and sets forth the custodian or custodian/location associated with each produced document. Hard-copy documents will be scanned using Optical Character Recognition (OCR) technology and searchable ASCII text files will be produced (or Unicode text format if the text is in a foreign language), unless the producing party can show that the cost would outweigh the usefulness of scanning (for example, when the condition of the paper is not conducive to scanning and will not result in accurate or reasonably useable/searchable ESI). Each file will be named with a unique Bates Number (e.g., the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

11. Exception Reporting. If any documents not otherwise identified as system or operating files, the producing party must disclose processing exceptions that are unresolved, such as documents that cannot be opened due to encryption or other processing issues.

E. Preservation of ESI

The parties acknowledge that they have an obligation, as expressed in Federal Rules of Civil Procedure, Rule 37(e), to take reasonable and proportional steps to preserve discoverable information in the party's possession, custody, or control. With respect to preservation of ESI, the parties agree as follows:

1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their possession, custody, or control.

2. The parties will supplement their disclosures in accordance with Federal Rules of Civil Procedure, Rule 26(c) with discoverable ESI responsive to a particular discovery request or mandatory disclosure.

3. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved:

a. Deleted, slack, fragmented, or other data only accessible by forensics.

b. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

c. On-line access data such as temporary internet files, history, cache, cookies, and similar files.

d. Data in metadata fields that are frequently updated automatically, such as last-opened dates (see also Section (E)(5)).

e. Back-up data that are duplicative of data that are more accessible elsewhere.

f. Server, system or network logs.

g. Data remaining from systems no longer in use that is unintelligible on the systems use.

h. Electronic data (*e.g.*, email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, Android devices), provided that a copy of all such electronic data is automatically saved elsewhere (such as a server, laptop, desktop computer, or "cloud" storage).

F. Privilege

1. A producing party shall create a privilege log of all documents fully withheld from production on the basis of a privilege or protection, unless otherwise agreed or accepted by this Stipulation and Order. Privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). For ESI, the privilege log may be generated manually or using available metadata, including author/recipient or to/from/cc/bcc names; the subject matter or title; and date created/sent/received.

a. Privilege logs will be produced to all other parties no later than 45 days after delivering a production, unless a different deadline is agreed to by the parties.

b. The privilege log shall conform with the requirements of the Federal Rules of Civil Procedure and. to the extent reasonably available, the privilege log shall identify for each claimed privileged document: (i) a description sufficient to allow the Parties to analyze the relevance and claimed privilege; (ii) the date of the document; (iii) author of the document; and (iv) the claimed basis for withholding the document.

2. Redactions need not be logged so long as the basis for the redaction is clear on the face of the redacted document.

3. With respect to privileged or work-product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs after September 15, 2023. Defendant will provide a blanket entry in its privilege log for materials withheld on the grounds of privilege and/or attorney work product between Brady Martz and its outside counsel about the data security incident at issue in this case dated on or after November 19, 2022.

4. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Federal Rules of Civil Procedure, Rule 26(b)(3)(A) and (B).

5. Pursuant to Federal Rules of Evidence 502(d), the production of any documents in this proceeding shall not, for the purposes of this proceeding or any other federal or state proceeding, constitute a waiver by the producing party of any privilege applicable to those documents, including the attorney-client privilege, attorney work-product protection, or any other privilege or protection recognized by law. Information produced in discovery that is protected as privileged or work product shall be immediately returned to the producing party after the receiving party is notified and the producing party has shown that it has taken reasonable steps to avoid inadvertent disclosures. Inadvertent privileged production of documents shall not constitute a waiver of such protection.

THEREFORE, the Court hereby issues an order entering and establishing this Stipulated ESI Protocol as set forth herein.

IT IS SO ORDERED.

Dated this 17th day of July, 2024.

/s/ Alice R. Senechal
Alice R. Senechal
United States Magistrate Judge